Manajemen Risiko Sistem Informasi Akademik pada Perguruan Tinggi Menggunakan Metoda Octave Allegro

Deni Ahmad Jakaria
Jurusan Teknik Informatika
STMIK DCI
Jl. Sutisna Senjaya No. 158A
Tasikmalaya, Indonesia
deni.ahmad.jakaria@gmail.com

R. Teduh Dirgahayu
Magister Informatika, Fakultas
Teknologi Industri
Universitas Islam Indonesia
Jl. Kaliurang Km. 14.4 Besi Sleman
Yogyakarta, Indonesia

Hendrik
Magister Informatika, Fakultas
Teknologi Industri
Universitas Islam Indonesia
Jl. Kaliurang Km. 14.4 Besi Sleman
Yogyakarta, Indonesia

***Abstrak*—Kesadaran akan pentingnya keamanan sistem informasi beserta aset-asetnya bagi suatu organisasi dan dampak yang mungkin timbul akibat kerusakan sistem informasi beserta asetnya tampaknya masih belum mendapatkan perhatian bagi sebagaian besar organisasi. Penilaian risiko merupakan bagian dari manajemen risiko sistem informasi, dilakukan untuk menilai seberapa besar kemungkinan adanya ancaman dan kerentanan terhadap sistem informasi beserta aset - asetnya. Penelitian ini bertujuan untuk melakukan analisis risiko pada sistem informasi akademik di perguruan tinggi. Hasil akhir dari penilaian risiko berupa rekomendasi mengenai langkah – langkah yang harus diambil untuk perlindungan sistem informasi beserta aset – asetnya.**

Kata kunci: analisis risiko, manajemen risiko

I. PENDAHULUAN

Teknologi web memberikan kemudahan untuk mengakses informasi cepat dan murah yang disediakan oleh website maupun pustaka digital. Selain manfaat berupa kecepatan dan kemudahan akses, teknologi web rentan terhadap sabotase, serta tindak kejahatan [1].

Pada saat ini banyak perguruan tinggi telah memanfaatkan teknologi web sebagai sarana untuk melayani mahasiswa dalam bidang akademik. Sifat teknologi web yang mudah diakses dan digunakan menjadi alasan utama beberapa perguruan tinggi memilihnya untuk pelayanan akademik.

Penelitian ini akan mengamati layanan akademik berbasis web pada salah satu Perguruan Tinggi. Penelitian ini memfokuskan pada identifikasi, analisis dan penilaian risiko Sistem Informasi Akademik berbasis web pada Perguruan Tinggi menggunakan metoda *OCTAVE Allegro.*

Saat ini belum banyak institusi yang melakukan *risk assessment* pada sistem informasi yang digunakan. Di satu sisi sistem informasi telah menjadi bagian yang sulit dipisahkan pada hampir setiap proses bisnis di institusi tersebut. Dengan demikian jika terdapat gangguan pada sistem informasi maka dapat mengganggu keberlangsungan proses bisnis institusi yang bersangkutan.

Beberapa penelitian menunjukkan bahwa sistem informasi beserta asetnya rentan terhadap risiko kerusakan fisik dan logik. Risiko kerusakan fisik berkaitan dengan perangkat keras seperti bencana alam (*natural disaster*), pencurian (*theft*), kebakaran (*fires*), lonjakan listrik (*power surge*) dan perusakan (*vandalism*). Risiko kerusakan logik mengacu kepada akses tidak sah (*unauthorized access*), kerusakan secara sengaja maupun tidak disengaja pada sistem informasi dan data [1] untuk itu perlu dilakukan identifikasi ancaman dan analisis risiko untuk meningkatkan keamanan dan mengurangi risiko kerusakan sistem informasi.

Dengan manajemen risiko teknologi informasi diharapkan dapat mengurangi dampak kerusakan yang bisa berupa: dampak terhadap financial, menurunnya reputasi disebabkan sistem yang tidak aman, terhentinya operasi bisnis, kegagalan aset yang dapat dinilai (sistem dan data) dan penundaan proses pengambilan keputusan [6].

Salah satu metoda yang digunakan untuk manajemen dan analisis risiko teknologi informasi adalah OCTAVE (*Operationally Critical Threat, Assets and Vulnerability Evaluation*). *OCTAVE* dikembangkan oleh *Software Engineering Institute (SEI)* Universitas Carnegie Mellon. *OCTAVE* merupakan seperangkat peralatan, teknik dan metode untuk penilaian dan perencanaan keamananan sistem informasi berbasis risiko. *OCTAVE* memiliki tiga varian yaitu *OCTAVE*, *OCTAVE-S* dan *OCTAVE Allegro*. *OCTAVE Allegro* memfokuskan pada aset informasi dan data yang mendukung informasi tersebut.

A. *Rumusan Masalah*

Rumusan masalah untuk penelitian ini adalah:

- Pihak manajemen mengalami kesulitan dalam menyampaikan pentingnya untuk menjaga sistem informasi beserta aset-asetnya dalam rangka menjaga keberlanjutan proses bisnis.
- Belum ada kebijakan mengenai pengelolaan sistem informasi.
- Belum pernah dilakukan penilaian risiko pada sistem informasi yang terdapat di universitas tersebut.

B. *Batasan Masalah*

Adapun batasan masalah pada penelitian ini adalah:

- Penilaian risiko difokuskan pada Sistem Informasi untuk melindungi aset-aset yang penting.
- Penilaian risiko dilakukan pada bagian Divisi TI yang bertanggungjawab dan mengelola Sistem Informasi Akademik.
- Metoda yang digunakan adalah OCTAVE Allegro.

C. Tujuan penelitian ini adalah:

- Untuk mengidentifikasi, menganalisis dan mengelola risiko Sistem Informasi Akademik pada Perguruan Tinggi menggunakan metoda OCTAVE Allegro.
- Mengembangkan strategi keamanan sistem informasi untuk meningkatkan keamanan sistem informasi.
- Membuat kebijakan manajemen risiko yang mendukung misi dan prioritas organisasi untuk mengurangi dampak kerugian akibat kerusakan sistem informasi.

D. Manfaat Penelitian

Manfaat yang ingin diperoleh dari penelitian ini adalah:

- Mengurangi risiko terjadinya kerusakan pada sistem informasi akademik beserta asetnya.
- Meningkatkan keamanan sistem informasi akademik.
- Mengurangi dampak kerugian akibat kerusakan sistem informasi akademik.
- Pihak manajemen dapat menekankan kepada karyawan mengenai pentingnya keamanan Sistem Informasi beserta aset – asetnya.
- Karyawan menyadari akan pentingnya menjaga keamanan Sistem Informasi dari kerusakan yang dapat menyebabkan terganggunya proses bisnis di perguruan tinggi yang bersangkutan

II. TINJAUAN PUSTAKA

Hasil penelitian sebelumnya [11] menyatakan bahwa proses peniliaian risiko perlu dilakukan secara berkala dan peran serta karyawan perlu ditingkatkan sehingga mereka menyadari pentingnya aset informasi, ancaman dan risiko yang mungkin terjadi serta konsekuensi yang harus mereka hadapi.

Beberapa tantangan yang mungkin dihadapi pada saat implementasi OCTAVE Allegro sebagai metodologi peniliaian risiko sistem informasi antara lain [2]:

- Perubahan Pola Pikir: Fokus Teknis menjadi Fokus Bisnis.
- Lingkungan Universitas dengan Struktur Konfederasi.
- Keterbukaan di Lingkungan Universitas.
- Penyesuaian dengan Pihak Ketiga.

A. Keamanan Sistem Informasi

Menurut SANS.org keamanan informasi mengacu pada proses dan metodologi yang dirancang dan dilaksanakan untuk melindungi informasi elektronik atau bentuk lainnya yang bersifat rahasia, informasi pribadi serta data yang sensitif dari akses yang tidak sah, penyalahgunaan, pengungkapan, perusakan dan modifikasi serta gangguan.

Prinsip utama keamanan sistem informasi terdiri dari *confidentiality* (kerahasiaan), *integrity* (integritas) dan *availability* (ketersediaan) atau sering disingkat CIA [8] seperti tampak pada gambar dibawah.

Gambar 1. CIA Triad [8]

B. Ancaman Keamanan Sistem Informasi

Menurut [8] ancaman (*threats*) merupakan setiap peristiwa yang jika terjadi, dapat menyebabkan kerusakan pada sistem dan membuat hilangnya kerahasiaan, ketersediaan, atau integritas. Ancaman bisa berbahaya - seperti modifikasi yang disengaja terhadap informasi sensitif - atau tidak disengaja - seperti kesalahan dalam perhitungan transaksi atau penghapusan file.

Sedangkan kerentanan (*vulnerability*) adalah kelemahan dalam sistem yang dapat dieksploitasi oleh ancaman. Mengurangi aspek kerentanan dari sistem dapat mengurangi risiko ancaman pada sistem.

Kerentanan dapat dinilai sesuai dengan tingkat risiko terhadap organisasi, baik secara internal maupun eksternal. Rating yang rendah dapat diterapkan untuk kerentanan dengan tingkat kerusakan dan paparan rendah.

C. Manajemen Risiko dan Penilaian Risiko

Bahwa manajemen risiko merupakan proses yang memungkinkan manajer TI untuk menyeimbangkan biaya operasional dan biaya ekonomi untuk tindakan pengamanan dalam upaya melindungi sistem IT dan data yang mendukung misi organisasi [4].

Suatu upaya dari perencanaan, pengorganisasian, memimpin dan mengendalikan sumber daya dan kegiatan untuk meminimalkan dampak dari kerugian akibat kecelakan pada biaya yang paling dapat diterima. Untuk memenuhi kebutuhan spesifik organisasi, keberhasilan manajemen risiko harus menyeimbangkan pengendalian risiko dan teknik risiko pembiayaan dengan mempertimbangkan visi, misi, nilai – nilai dan tujuan organisasi [3].

Manajemen risiko secara umum merupakan proses dengan tujuan untuk mendapatkan keseimbangan antara efisiensi dan merealisasikan peluang untuk mendapatkan keuntungan dan meminimalkan kerentanan dan kerugian. Manajemen risiko harus menjadi proses tanpa henti dan berulang yang terdiri dari beberapa fase, ketika diterapkan dengan benar, memungkinkan terjadinya perbaikan terus-menerus dalam pengambilan keputusan dan peningkatan kinerja [5].

Penilaian risiko (*risk assessment*) merupakan bagian dari manajemen risiko, penilaian risiko adalah proses untuk menilai

seberapa sering risiko terjadi atau seberapa besar dampak dari risiko [6].

Tujuan utama melakukan analisis risiko adalah untuk mengukur dampak dari potensi ancaman, menentukan berapa besar kerugian yang diderita akibat hilangnya potensi bisnis. Hasil utama dari analisis risiko dua diantaranya adalah identifikasi risiko dan jumlah biaya berbanding manfaatnya untuk penanggulangan risiko kerusakan.

Manfaat melakukan analisis risiko antara lain menciptakan rasio *cost-to-value* yang jelas untuk perlindungan keamanan. Hal ini juga mempengaruhi proses pengambilan keputusan yang berhubungan dengan konfigurasi hardware dan desain sistem software [8].

Tujuan dari penilaian risiko adalah untuk melakukan identifikasi: (i) ancaman terhadap organisasi (contoh: operasional, aset atau individu) atau ancamana yang dialamatkan melalui organisasi kepada organisasi lain atau negara; (ii) kerentanan pada organisasi baik dari internal maupun eksternal; (iii) Bahaya terhadap organisasi yang mungkin terjadi yang diakibatkan oleh eksploitasi kerentanan; (iv) kemungkinan terjadinya bahaya atau kerusakan [5].

Hasil akhir dari analisis risiko adalah penentuan risiko (contoh: tingkat bahaya dan kemungkinan dari bahaya yang terjadi). Untuk mendukung komponen penilaian risiko, organisasi harus melakukan identifikasi antara lain: (i) alat, teknik, dan metodologi yang digunakan untuk menilai risiko, (ii) asumsi terkait dengan penilaian risiko, (iii) kendala yang dapat mempengaruhi penilaian risiko; (iv) peran dan tanggung jawab; (v) bagaimana risiko informasi penilaian dikumpulkan, diproses dan dikomunikasikan ke seluruh organisasi, (vi) bagaimana penilaian risiko yang dilakukan dalam organisasi, (vii) frekuensi penilaian risiko, dan (viii) bagaimana informasi ancaman diperoleh (yaitu, sumber dan metode).

Dalam melakukan analisis risiko terdapat tiga langkah utama, analisis risiko umumnya jauh lebih komprehensif dan dirancang untuk digunakan agar dapat mengukur tingkat kerumitan dalam skenario multi risiko.

Langkah – langkahnya adalah sebagai berikut [8]:

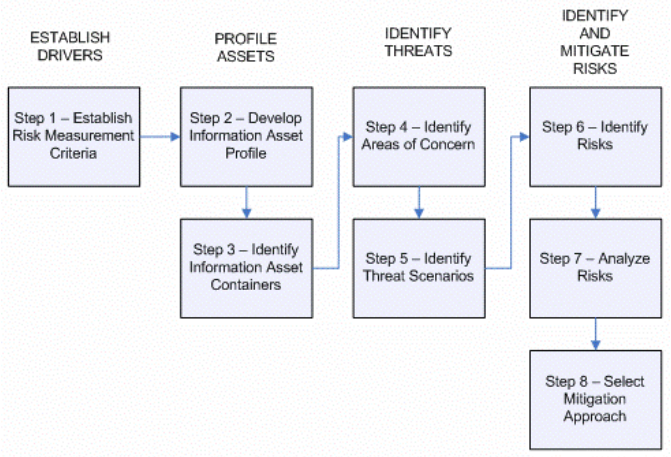
- Perkirakan potensi kerugian pada aset dengan menentukan nilai masing-masing aset.
- Melakukan analisis potensi ancaman terhadap aset.
- Tentukan *Annualized Loss Expectancy* (ALE).

D. Metoda OCTAVE

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) mendefinisikan komponen-komponen penting secara komprehensif, sistematis, berbasis konteks (context-driven) evaluasi risiko keamanan informasi. Dengan menggunakan metode OCTAVE, organisasi dapat membuat perlindungan terhadap informasi berbasis pengambilan keputusan risiko berdasarkan CIA (*Confidentiality, Integrity, Authentication*) untuk aset teknologi informasi kritis [9].

OCTAVE merupakan metodologi untuk mengidentifikasi dan mengevaluasi risiko keamanan sistem informasi. Penggunaan OCTAVE ditujukan untuk membantu organisasi dalam hal: (a) Mengembangkan kriteria evaluasi risiko kualitatif yang menggambarkan toleransi risiko operasional organisasi; (b) Mengidentifikasi aset – aset penting untuk mencapai misi organisasi; (c) Mengidentifikasi kerentanan dan ancaman terhadap aset tersebut; (d) Menentukan dan melakukan evaluasi untuk menghadapi konsekuensi yang terjadi pada organisasi jika ancaman tersebut terjadi.

Metoda OCTAVE memiliki tiga varian yaitu OCTAVE, OCTAVE-S dan OCTAVE Allegro. *OCTAVE* merupakan seperangkat peralatan, teknik dan metode untuk penilaian dan perencanaan keamananan sistem informasi berbasis risiko. OCTAVE Allegro merupakan metoda yang disederhanakan dengan fokus pada aset informasi. OCTAVE Allegro dapat dilakukan dengan metoda workshop-style dan kolaboratif. OCTAVE Allegro terdiri dari delapan langkah dibagi dalam empat fase.



Gambar 2. Langkah – langkah OCTAVE Allegro [7]

III. TAHAPAN PENILAIAN RISIKO

A. Langkah 1 – Membangun Kriteria Pengukuran Risiko

Langkah ini terdapat dua aktivitas, diawali dengan membangun *organizational drivers* digunakan untuk mengevaluasi dampak risiko pada misi dan tujuan bisnis, serta mengenali *impact area* yang paling penting. Aktivitas 1 yaitu membuat definisi ukuran kualitatif yang didokumentasikan pada *Risk Measurement Criteria Worksheets*. Aktivitas dua melakukan pemberian nilai prioritas *impact area* menggunakan *Impact Area Ranking Worksheet*.

B. Langkah 2 – Mengembangkan Profil Aset Informasi

Terdiri dari delapan aktivitas, diawali dengan identifikasi aset informasi selanjutnya dilakukan penilaian risiko terstruktur pada aset yang kritis. Aktivitas tiga dan empat mengumpulkan informasi mengenai information aset yang penting dilanjutkan dengan membuat dokumentasi alasan pemilihan aset informasi kritis. Aktivitas lima dan enam membuat deskripsi aset informasi kritis kemudian mengidentifikasi kepemilikan dari aset informasi kritis tersebut. Aktivitas tujuh mengisi kebutuhan keamanan untuk *confidentiality*, *integrity* dan *availaibility*. Aktivitas delapan mengidentifikasi kebutuhan keamanan yang paling penting untuk aset informasi.

C. Langkah 3 – Mengidentifikasi Kontainer dari Aset Informasi

Hanya ada satu aktivitas pada langkah tiga, perhatikan tiga poin penting terkait dengan keamanan dan konsep dari kontainer aset informasi yaitu cara aset informasi dilindung, tingkat perlindungan atau pengaman aset informasi dan kerentanan serta ancaman terhadap kontainer dari aset informasi.

D. Langkah 4 – Mengidentifikasi Area Masalah

Aktivitas pada langkah empat yaitu diawali dengan pengembangan profil risiko dari aset informasi dengan cara bertukar pikiran untuk mencari komponen ancaman dari situasi yang mungkin mengancam aset informasi. Dengan berpedoman pada dokumen *Information Asset Risk Environment Maps* dan *Information Asset Risk Worksheet* maka dapat dicatat *area of concern*. Berpedoman pada dokumen *Information Asset Risk Worksheet* lakukan review dari kontainer untuk membuat *Area of Concern* dan mendokumentasikan setiap *Area of Concern.*

E. Langkah 5 – Mengidentifikasi Skenario Ancaman

Aktivitas satu pada langkah lima yaitu melakukan identifikasi skenario ancaman tambahan pada aktivitas ini dapat menggunakan *Appendix C – Threat Scenarios Questionnaries*. Aktivitas dua melengkapi *Information Asset Risk Worksheets* untuk setiap *threat scenario* yang umum.

F. Langkah 6 – Mengidentifikasi Risiko

Aktivitas satu pada langkah 6 menentukan threat scenario yang telah didokumentasikan di *Information Asset Risk Worksheet* dapat memberikan dampak bagi organisasi.

G. Langkah 7 – Menganalisis Risiko

Aktivitas harus dilakukan mengacu pada dokumentasi yang terdapat pada *Information Asset Risk Worksheet.* Aktivitas satu dimulai dengan melakukan review *risk measurement criteria* dilanjutkan dengan aktivitas kedua menghitung nilai risiko relatif yang dapat digunakan untuk menganalisis risiko dan memutuskan strategi terbaik dalam menghadapi risiko.

H. Langkah 8 – Memilih Pendekatan Pengurangan

Aktivitas satu pada langkah delapan yaitu mengurutkan setiap risiko yang telah diidentifikasi berdasaarkan nilai risikonya. Hal ini dilakukan untuk membantu dalam pengambilan keputusan status mitigasi risiko tersebut. Aktivitas dua melakukan pendekatan mitigasi untuk setiap risiko dengan berpedoman pada kondisi yang unik di organisasi tersebut.

IV. PEMBAHASAN

Tahap pertama pelaksanaan penilaian risiko dimulai dengan menghubungi pihak – pihak pengelola di divisi TI antara lain pimpinan divisi, sistem analis serta programmer untuk mendapatkan data – data yang diperlukan. Tahap selanjutnya adalah melakukan wawancara untuk mendapatkan informasi mengenai aset operational kritis bagi organisasi.

Langkah 1 - setelah membangun *organizational drivers* maka dilakukan penentuan *impact area* yang paling penting serta memberikan nilai skala prioritas pada *impact area* yang telah ditentukan. Sebagai pertimbangan untuk menentukan *impact area* adalah misi dan tujuan bisnis organisasi tersebut. Prioritas *impact area* yang dipilih pertama adalah reputasi dan kepercayaan pelanggan, finansial, produktivitas, keamanan dan kesehatan serta denda dan penalti. Tabel 1 berisi hasil penentuan *impact area* – reputasi dan kepercayaan pelanggan dan tabel 2 adalah skala prioritas *impact area*.

TABEL I. IMPACT AREA – REPUTASI DAN KEPERCAYAAN PELANGGAN

Impact Area	Low	Medium	High
Reputation	Reputasi sedikit terpengaruh; tidak ada usaha atau dibutuhkan usaha kecil untuk perbaikan	Reputasi terkena dampak buruk, dan dibutuhkan usaha dan biaya untuk perbaikan	Reputasi terkena dampak sangat buruk hingga hampir tidak dapat diperbaiki
Customer Loss	Kurang dari 2% pengurangan pelanggan yang diakibatkan hilangnya kepercayaan	2% hingga 10% pengurangan pelanggan yang diakibatkan hilangnya kepercayaan	Lebih dari 10% pengurangan pelanggan yang diakibatkan hilangnya kepercayaan

TABEL II. SKALA PRIORITAS IMPACT AREA

Priority	Impact Areas
5	Reputasi dan kepercayaan pelanggan
4	Finansial
3	Produktivitas
1	Keamanan dan Kesehatan
2	Denda dan Penalti

Langkah 2 - Dalam mengembangkan *information asset profile* harus ditentukan aset informasi kritis berdasarkan *core process* dari organisasi tersebut, yaitu dimulai dari data mahasiswa hingga laporan nilai akhir berbentuk transkrip. Aktivitas selanjutnya yaitu menentukan aset informasi kritikal yang dicatat pada *critical asset information worksheet.* Aset informasi yang dipilih harus mempertimbangkan hal – hal berikut:

- Aset informasi yang penting dan digunakan dalam kegiatan sehari – hari.
- Aset informasi yang jika hilang dapat mengganggu tujuan dan misi organisasi.

Dari hasil pertimbangan di atas maka informasi yang dikategorikan sebagai aset informasi penting diantaranya yaitu profil mahasiswa, profil dosen, profil mata kuliah dan transaksi nilai mahasiswa. Tabel 3 berisi contoh *information asset profiling* untuk transaksi nilai mahasiswa.

TABEL III. INFORMATION ASSET PROFILLING – TRANSAKSI NILAI MAHASISWA

Critical Asset	Transaksi nilai mahasiswa
Rationale for Selection	Digunakan untuk menentukan IPK dan penentuan mutu mahasiswa
Description	Terdiri dari nilai akhir mahasiswa
Owner	Manajer

Security Requirements	**Confidentiality**	Informasi nilai sangat penting bagi mahasiswa, dosen & jurusan. Bagian administrasi mahasiswa menggunakan informasi untuk mencetak transkrip nilai
	Integrity	Informasi harus benar dan akurat, dapat berubah dan diganti oleh dosen, hanya operator di bagian administrasi kemahasiswaan yang dapat memasukan atau memodifikasi nilai mahasiswa
	Availability	Informasi harus selalu tersedia bagi mahasiswa, dosen dan bagian administrasi kemahasiswaan
Most Important Security Requirement		**Integrity** **Alasan:** Nilai merupakan informasi penting bagi mahasiswa, jika terdapat kesalahan akan merugikan mahasiswa

Langkah 3 - Identifikasi *information asset container* yang terbagi menjadi tiga yaitu *technical*, *physical* dan *people* masing – masing memiliki sisi eksternal dan internal dibantu menggunakan worksheet *Information Asset Risk Environment Map*. Tabel 4 berisi contoh *Information Asset Risk Environment Map (Technical)* – Transaksi Nilai Mahasiswa.

TABEL IV. INFORMATION ASSET RISK ENVIRONMENT (TECHNICAL) – TRANSAKSI NILAI MAHASISWA

Data Transaksi Nilai Mahasiswa	
Information Asset Risk Environment Map (Technical)	
Internal	
Container Description	**Owner(s)**
Modul: Transaksi Input Nilai Input transaksi nilai mahasiswa untuk proses pengolahan nilai mahasiswa.	Administrasi Kemahasiswaan, Staff Jurusan
External	**Owner(s)**
Container Description	Mahasiswa
Aplikasi: Web Nilai	
Mahasiswa dapat melihat nilai	

Langkah 4 – Identifikasi *areas of concern* dengan meninjau kembali setiap *container* untuk melihat dan menentukan *areas of concern* yang potensial dilanjutkan dengan melakukan dokumentasi setiap *areas of concern* yang telah diidentifikasi. *Areas of concern* diperluas untuk mendapatkan *threat scenarios* kemudian didokumentasikan untuk melihat apakah mempengaruhi *security requirements*. Tabel 5 berisi contoh *area of concern* transaksi nilai mahasiswa.

TABEL V. AREA OF CONCERN – TRANSAKSI NILAI MAHASISWA

No	Area of Concern
1	Jumlah data nilai yang banyak dapat menyebabkan kesalahan input data oleh staff administrasi kemahasiswaan
2	Penyebaran akses password transaksi nilai oleh staff bagian administrasi yang memiliki akses
3	Celah keamanan pada aplikasi web nilai mahasiswa yang dapat dieksploitasi oleh pihak dalam/luar
4	*Error* yang terjadi pada saat proses insert/update/delete modul transaksi nilai dilakukan secara bersama-sama

Langkah 5 – Identifikasi *threat scenario* yang memberikan gambaran secara rinci mengenai *property* dari *threat*, antara lain *actor, means, motives, outcome* dan *security requirement.* Melengkapi *Information Asset Risk Worksheets* untuk setiap *threat scenario* yang umum. Tabel 6 merupakan contoh *properties of threat* hasil perluasan dari *areas of concern* transaksi nilai mahasiswa.

TABEL VI. PROPERTIES OF THREAT – TRANSAKSI NILAI MAHASISWA

	Area of Concern	**Threat of Properties**	
1	Jumlah data nilai yang banyak menyebabkan kesalahan input data nilai oleh staff administrasi kemahasiswaan	**1. Actors**	Staff administrasi kemahasiswaan
		2. Means	Staff menggunakan modul aplikasi nilai mahasiswa
		3. Motives	*Human error (accidental)*
		4. Outcome	*Modification, interruption*
		5. Security Requirements	- Validasi input data nilai pada field - Dosen atau Staff Jurusan melakukan verifikasi nilai yang telah diinput oleh staff administrasi kemahasiswaan
2	**Area of Concern**	**Threat of Properties**	
	Penyebaran akses password transaksi nilai oleh staff administrasi kemahasiswaan yang memiliki akses	**1. Actors**	Staff administrasi
		2. Means	Modul aplikasi nilai mahasiswa
		3. Motives	Secara sengaja/tidak sengaja memberitahukan password (*deliberate, accidental*)
		4. Outcome	*Disclosure, Modification, Interruption*
		5. Security Requirements	Memberikan pemahaman untuk menjaga kerahasiaan password dan hukuman bagi staff yang sengaja menyebarkan password

Langkah 6 – Identifikasi risiko bertujuan untuk menentukan bagaiman *threat scenario* memberikan dampak bagi organisasi serta menentukan tingkatannya apakah *high*, *medium* atau *low*. Dilanjutkan dengan menghitung *relative score* untuk membantu organisasi dalam menganalisis risiko serta menentukan strategi yang tepat untuk menghadapi risiko. Tabel 7 menunjukan cara menghitung *relative score*.

TABEL VII. MENGHITUNG SCORE IMPACT AREA

Impact areas	**Priority**	**Low (1)**	**Medium (2)**	**High (3)**
Reputasi dan kepercayaan pelanggan	**5**	**5**	**10**	**15**
Finansial	**4**	**4**	**8**	**12**

Produktivitas	**3**	**3**	**6**	**9**
Keamanan dan Kesehatan	**1**	**1**	**2**	**3**
Denda dan Penalti	**2**	**2**	**4**	**6**

Langkah 7 - Analisis risiko dilakukan pada setiap *area of concern* dari *information asset* serta konsekuensi yang terjadi berdasarkan *relative risk score*. Dibawah ini adalah tabel contoh analisis risiko – transaksi nilai mahasiswa.

TABEL VIII. ANALISIS RESIKO – TRANSAKSI NILAI MAHASISWA

Area of concern	***Risk***			
Jumlah data nilai yang banyak menyebabkan kesalahan input data nilai oleh staff administrasi kemahasiswaan	**Consequences**	Diperlukan waktu tambahan untuk memperbaiki kesalahan input data nilai		
	Severity	**Impact Area**	**Value**	**Score**
		Reputasi dan kepercayaan pelanggan	Med	10
		Finansial	Low	4
		Produktivitas	High	9
		Keamanan dan Kesehatan	Low	1
		Denda dan Penalti	Low	2
		Relative Risk Score		26

Langkah 8 – Pemilihan pendekatan mitigasi dilakukan berdasarkan pengelompokan risiko. Tabel 9 memperlihatkan contoh pengelompokkan langkah mitigasi berdasarkan *Relative Risk Matrix*, pada tabel 10 merupakan pengelompokkan langkah mitigasi, tabel 11 adalah contoh mitigasi risiko berdasarkan *area of concern*.

TABEL IX. RELATIVE RISK MATRIX

RISK SCORE		
30 TO 45	**16 TO 29**	**0 TO 15**
POOL 1	POOL 2	POOL 3

TABEL X. TABEL VIII. MITIGATION APPROACH

Pool	**Mitigation Approach**
Pool 1	Mitigate
Pool 2	Mitigate or Defer
Pool 3	Accept

TABEL XI. TABEL IX. CONTOH MITIGASI RISIKO BERDASARKAN AREA OF CONCERN

Risk Mitigation	
Area of Concern	Jumlah data nilai yang banyak menyebabkan kesalahan input data nilai oleh staff administrasi kemahasiswaan
Action	Mitigate
Container	Control
Modul data nilai mahasiswa	Dibuat validasi input pada field tertentu
Staff Jurusan / Dosen	Dosen atau staff jurusan dapat melakukan verifikasi nilai yang telah diinputkan oleh staff administrasi kemahasiswaan

V. KESIMPULAN

OCTAVE Allegro merupakan salah satu metoda manajemen risiko sistem informasi yang dapat diterapkan pada perguruan tinggi tanpa memerlukan keterlibatan yang ekstensif di dalam organisasi dan difokuskan pada aset informasi yang kritis bagi keberlangsungan organisasi dalam mencapai misi dan tujuannya.

Penilaian risiko dapat memberikan gambaran mengenai kemungkinan adanya ancaman pada aset kritikal dan mengambil langkah – langkah pencegahan yang tepat untuk meminimalkan kemungkinan ancaman tersebut terjadi.

Dari hasil penilaian risiko maka pembuat kebijakan dapat membuat perencanaan strategis untuk menjaga aset informasi kritikal secara tepat serta langkah – langkah pemulihan jika skenario ancaman benar – benar terjadi.

DAFTAR PUSTAKA

[1] A. M. Suduc, M. Bîzoi dan F. G. Filip. (2010). Audit for Information Systems Security. Journal Informatica Economică, 14(1),43-48.

[2] E. Goldman (2009). Challenges and Concerns for Implementing OCTAVE Allegro in a University Environment. http://www.ericgoldman.name/security/2-enterprise-security/14-challenges-and-concerns-for-implementing-octave-allegro-in-a-university-environment di akses tanggal 18 Maret 2013.

[3] G. Blokdijk, C. Engle, J. Brewster. (2008). IT Risk Management Guide: Risk Management Implementation Guide, Presentations, Blueprints, Templates. AU: Emereo Pty Limited.

[4] G. Stoneburner, A. Goguen dan A. Feringa. (2002). Risk Management Guide for Information Technology Systems. Recommendation of National Institute of Standards and Technology Special Publication 800-30.

[5] Joint Task Force Transformation Initiative (2011). Managing Information Security Risk: Organization, Mission, and Information System View. NIST Special Publication 800-39.

[6] M. M. Maulana dan S. H. Supangkat. (2006). Pemodelan Framework Manajemen Risiko Teknologi Informasi Untuk Perusahaan di Negara Berkembang. Prosiding Konferensi Nasional Teknologi Informasi & Komunikasi untuk Indonesia, 121-126.

[7] Richard. A. Caralli. (2007). Introducing OCTAVE Allegro: Improving the Information Securiy Risk Assessment Process. http://www.sei.cmu.edu/pub/documents/07.reports/07tr012.pdf. Diakses 7 September 2012.

[8] R. L. Krutz dan D. R. Vines. (2006). The CISSP Prep Guide - Mastering the Ten Domains of Computer Security. CA: Wiley Computer Publishing John Wiley & Sons, Inc

[9] S. K. Pandey dan K. Mustafa. (2012). A Comparative Study of Risk Assessment Methodologies for Information Systems. Buletin Teknik Elektro dan Informatika, 1(2),111-122.

[10] Technical Department of ENISA Section Risk Management (2006). Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools. ENISA.

[11] Welly dan Mikewati. (2011). Penilaian Resiko Sistem Informasi Pada Bina Nusantara Menggunakan Metode Octave Allegro. http://library.binus.ac.id/Collections/ethesis_detail/TSA-2012-0023.